De betekenis van IT-auditing voor de jaarrekeningcontrole ontrafeld!

Stan van Bommel, Mark van Goor, Lucien Peek en Joop Winterink

SAMENVATTING In dit artikel wordt beschreven op welke wijze een effectieve vertaalslag kan worden gemaakt om de impact van IT-controlebevindingen op de jaarrekeningcontrole te bepalen. Een adequate controleaanpak en samenwerking tussen de accountant en IT-auditor staan hierbij centraal. Door de inzet van een IT-auditor betekent het voor de accountant vooral dat de jaarrekeningcontrole efficiënter kan worden uitgevoerd. Daarnaast zijn de IT-controlebevindingen vooral de moeite waard voor het accountantsverslag en de managementletter van de accountant.

1 Inleiding

In het kader van de jaarrekeningcontrole werkt de accountant in toenemende mate met gegevens uit geautomatiseerde informatiesystemen. Voor de beoordeling van op informatietechnologie (IT) gebaseerde controlemaatregelen in het financiële verantwoordingsproces is specialistische kennis van IT en IT-beheersing nodig. Daarom schakelt de accountant de IT-auditor in. De IT-auditor voert General IT-controls onderzoeken uit en rapporteert aan de accountant die kennis neemt van de IT-controlebevindingen. Op basis hiervan kan de accountant efficiënt zijn controle naar user controls en application controls inrichten.

In de praktijk blijkt telkens weer dat de samenwerking tussen accountant en IT-auditor verre van optimaal is (onder andere Neisingh, 2002; NOREA, 2005; Fijneman, 1999) en ontbreekt veelal een concrete vertaalslag van de IT-controlebevinding naar de betekenis voor de jaarrekeningcontrole. Enerzijds begrijpt de accountant de betekenis van de IT-controlebevindingen voor de jaarrekeningcontrole onvoldoende en anderzijds lukt het de IT-auditor niet om het belang van zijn IT-controlebevindingen voor de jaarrekeningcontrole duidelijk te maken. De volgende voorbeelden illustreren de problematiek waarmee accountants en IT-auditors worstelen tijdens jaarrekeningcontroles.

Voorbeelden: De accountant doet onderzoek naar het factureringsproces om de volledigheid van de post premies in de jaarrekening vast te stellen. In welke mate laat de accountant de IT-auditor de logging van de applicatie Coda en de server onderzoeken? De logging geeft belangrijke informatie over de beveiliging van factureringsgegevens voor het doorbreken van (soms) onvervangbare beheersmaatregelen ten aanzien van functiescheiding en de integriteit van de audittrail. En wat als de accountant van mening is dat het factureringsproces betrouwbaar is, maar de IT-auditor geeft aan dat niet op het Change Management proces kan worden gesteund? Reden hiervoor kan zijn dat niet kan worden vastgesteld dat alle wijzigingen geautoriseerd in productie zijn genomen. Een onge-

C.F. van Bommel RE en L.C. Peek RE zijn als IT-auditors werkzaam bij de afdeling Internal Audit van de PGGM. Zij houden zich onder andere bezig met het uitvoeren van interne risk based audits op IT-gebied. Daarnaast zijn zij betrokken bij uitvoeren van IT-auditwerkzaamheden in het kader van de jaarrekeningcontrole ten behoeve van de externe accountant. J.A.W. Winterink RA RE is afdelingshoofd van Internal Audit en is als docent verbonden aan de postdoctorale opleiding EDP-auditing van de TIAS. Drs. H.M. van Goor RE CISA is werkzaam als Operational Risk Manager bij AEGON Nederland N.V. Hij houdt zich onder andere bezig met het monitoren en analyseren van (operationele) risico's en het definiëren, beheren en beoordelen van de interne controlemaatregelen in de operationele processen. Daarnaast is hij verantwoordelijk voor het bewaken van de SOX-compliancy binnen de unit Financial Services. Ook nu willen de auteurs, met hun derde artikel, een bijdrage leveren aan de verdere professionalisering van IT-vakgebied in relatie tot de jaarrekeningcontrole. Zij houden zich aanbevolen voor uw reacties en verdere discussie over dit belangrijke onderwerp.

autoriseerde wijziging kan niet gestructureerd zijn verlopen en is daarmee een risico voor de betrouwbaarheid en continuïteit van het factureringsproces.

Dit is het derde artikel in een reeks die antwoorden moet geven op dergelijke vragen uit de voorbeelden. Aanleiding voor het schrijven van de artikelen zijn onze ervaringen en de vernomen ervaringen van vakgenoten met het ontbreken van een duidelijke uitleg en benadering van begrippen als General IT-controls, betrouwbaarheid en continuïteit, alsmede de afbakening van IT-auditwerkzaamheden in het kader van de jaarrekeningcontrole. Een oorzaak hiervan is het ontbreken van eenduidige literatuur, definities en terminologie. Daarnaast hebben op IT-gebied zodanige ontwikkelingen plaatsgevonden dat de theorie niet meer volledig aansluit op de huidige praktijk. Het eerste artikel (Van Bommel en Van Goor, 2004) onderbouwt de aanleiding en beschrijft een methode voor de IT-auditor om samen met de accountant te komen tot een analyse van de te beoordelen General IT-controls. Het tweede artikel (Van Bommel en Van Goor, 2005) beschrijft aan de hand van een concreet praktijkvoorbeeld de uitwerking van de methode waarmee accountant én IT-auditor komen tot onderbouwingen van te onderzoeken General IT-controls.

De opzet van dit artikel is als volgt. In paragraaf 2 beschrijven wij in theorie hoe een vertaalslag van IT-controlebevinding naar de jaarrekeningposten wordt gemaakt. Daarna volgen in paragraaf 3 twee voorbeelden van General IT-controls onderzoeken. De betekenis van de bevindingen uit deze onderzoeken en de impact hiervan op de jaarrekeningcontrole en de jaarrekening wordt in paragraaf 4 beschreven. Vervolgens sluiten wij af met onze conclusies in paragraaf 5.
Ten behoeve van de leesbaarheid geven wij in figuur 1 de relaties tussen de gehanteerde begrippen in het artikel weer.

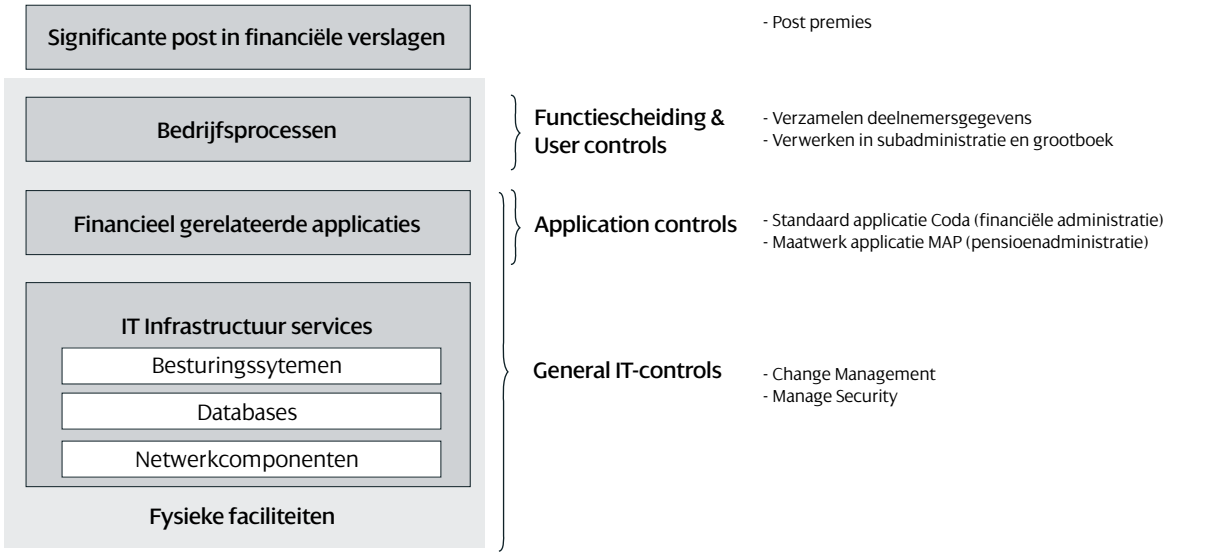
Een vierde artikel is in voorbereiding. Het vierde artikel vertaalt de IT-controlebevindingen van de IT-auditor naar de betekenis voor IT-governance en risicobeheersing door het management. Hierin ligt vooral de betekenis van IT-auditing. Al zijn de gevolgen van IT-controlebevindingen voor de jaarrekeningcontrole beperkt. Het maken van een effectieve vertaalslag van de IT-controlebevindingen is immers essentieel voor het management om de impact op de risicobeheersing in complexe IT-omgevingen te kunnen inschatten.

2 De vertaalslag in theorie

De accountant stelt zijn controleaanpak op. Samen met een IT-auditor stelt hij een overzicht op met de relaties tussen de jaarrekeningposten, de bedrijfsprocessen, de applicaties en de IT. Op basis van een risicoanalyse bepaalt de accountant de onderzoeken voor het desbetreffende jaar. De IT-auditor start met het uitvoeren van de General IT-controls-onderzoeken, zodat de accountant kan steunen op de IT-controlebevindingen. Vervolgens kan de accountant zijn onderzoeken efficiënt inrichten.

Om een vertaalslag van IT-controlebevindingen naar

Figuur 1 Relatie tussen gehanteerde begrippen in het artikel en de voorbeelden



de jaarrekeningposten te maken, is inzicht in de relatie tussen IT-component en jaarrekeningpost noodzakelijk. Dit inzicht hebben wij reeds eerder (Van Bommel en Van Goor, 2005) opgesteld in het kader van onze methode voor het selecteren van General IT-controls. Hierbij maken wij onderscheid naar IT-componenten, ondersteunende financiële applicaties en (sub-)processen.

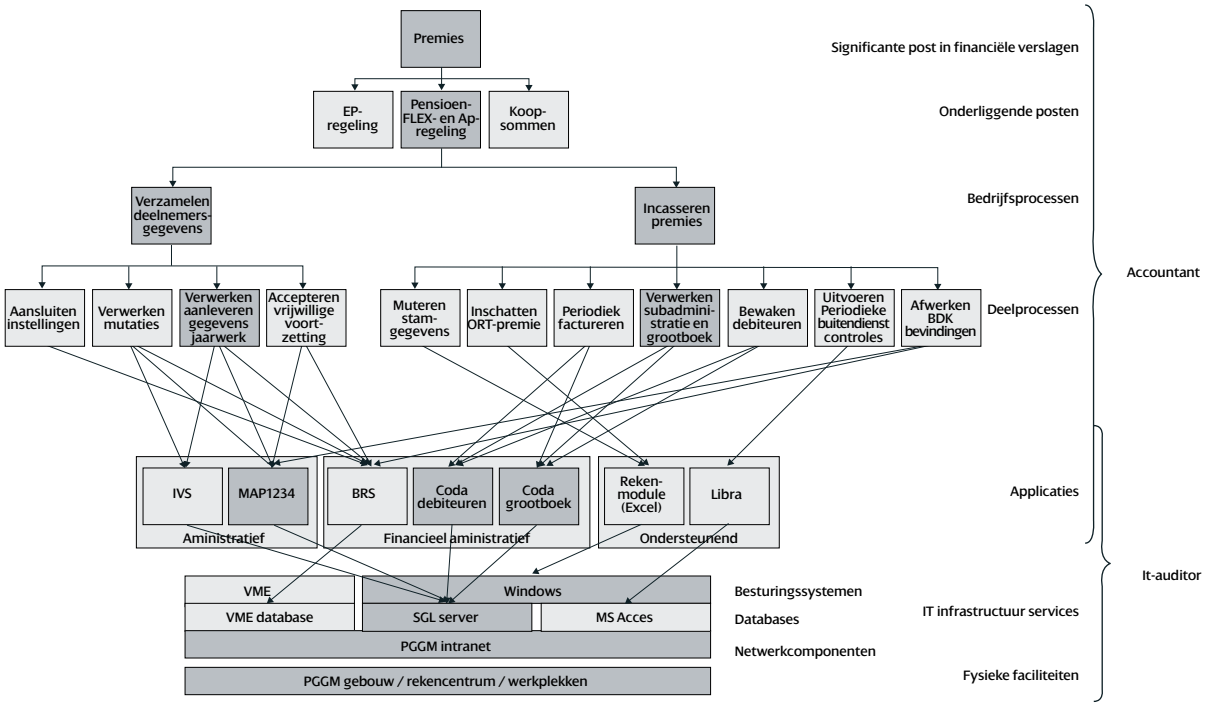
De analyse in het kader van het selecteren van General IT-controls van de jaarrekeningposten vindt topdown plaats (van jaarrekeningpost naar IT), terwijl de analyse van controlebevindingen voor de jaarrekeningcontrole bottom-up plaatsvindt (van IT naar jaarrekeningpost). In figuur 2 is een voorbeeld gegeven van de ontleding van de post premie-inkomsten bij een pensioenfonds. De figuur geeft een uitwerking van de post premies. Van de post premies is het onderdeel 'Pensioenen, FLEX- en AP-regeling' uitgewerkt. Deze post bestaat uit de deelprocessen 'verzamelen deelnemersgegevens' en 'incasseren premies'. Het doel van het proces 'verzamelen deelnemersgegevens' is het actueel houden van de gegevens die voor het factureringsproces van belang zijn. Onder meer na afloop van een jaar vindt verwerking van de aangeleverde definitieve gegevens inzake aangesloten instellingen en deelnemers plaats, het zogenaamde jaarwerk. Het doel van het proces 'incasseren premies' is het borgen dat premies juist, volledig en tijdig worden geïnd bij instellingen en deelnemers. Zo wordt onder meer periodiek aan de instellingen gefactureerd. De facturen worden verwerkt in de subadministratie en in het grootboek. Om de processen 'verzamelen deelnemergegevens' en 'incasseren premies' te kunnen uitvoeren, wordt gebruik gemaakt van de volgende applicaties:

- MAP (maatwerkapplicatie ten behoeve van pensioenadministratie);
- Coda (standaardapplicatie ten behoeve van financiële administratie).

Aan de hand van de risicoanalyse (NIVRA, 2005) door de accountant wordt onderscheid gemaakt naar het belang van processen. In figuur 2 zijn de kritieke componenten binnen de jaarrekeningpost 'Premies' met donkergrijs weergegeven. Op deze componenten zullen de IT-auditor en de accountant met name hun controlewerkzaamheden richten. De IT-auditor zal bij het uitvoeren van audits naar General IT-controls de donkergrijze componenten meenemen om de werking van beheersmaatregelen vast te stellen.

Het inzicht in de relaties tussen componenten laat zien dat een IT-controlebevinding niet los van een jaarrekeningpost kan staan. Door de IT-controle-

Figuur 2 Analyse van controlewerkzaamheden door de IT-auditor



bevinding te interpreteren naar de gevolgen voor applicaties en vervolgens voor het proces, kan een afgewogen oordeel plaatsvinden op het niveau van jaarrekeningposten.

3 Voorbeelden

Binnen het factureringsproces wordt een standenregister bijgehouden. Hiermee kan aansluiting worden gemaakt met het pensioensysteem. Vanuit efficiencyoogpunt onderzoekt de IT-auditor in overleg met de accountant de werking van een application control die garandeert dat er volledig wordt gefactureerd. De werking van de application control dient één keer te worden vastgesteld. Als blijkt dat de application control niet juist werkt, dan kan alsnog zekerheid worden verkregen door het uitvoeren van een steekproef naar de volledigheid van de verwerking van de facturering in het pensioensysteem.

Hierna werken wij twee fictieve voorbeelden uit van onderzoeken naar de General IT-controls. Uitgangspunt is dat de accountant een opdracht heeft gegeven aan de IT-auditor, zodat de accountant de volledigheid van de verantwoording van de post premies kan vaststellen. De accountant en IT-auditor maken hierbij een vertaling van IT-controlebevindingen naar het belang voor de jaarrekeningcontrole. Het eerste voorbeeld betreft de General IT-control Manage Changes. In dit voorbeeld leidt de IT-audit tot een negatief oordeel, zodat de accountant niet kan steunen op de IT. Het voorbeeld betreft specifiek de applicatie MAP en het bedrijfsproces 'Verwerken aanlevering gegevens jaarwerk'. Het tweede voorbeeld betreft de General IT-control Manage Security. In dit voorbeeld leidt de IT-audit tot een voldoende oordeel, maar met gewenste verbeteringen.

3.1 Voorbeeld 1 - Change Management

Het risico

Het proces Change Management is bedoeld om wijzigingen, gerelateerd aan de infrastructuur en applicaties, op een gecontroleerde wijze in productie te nemen. Change Management loopt vanaf het indienen van een wijzigingsverzoek tot en met de implementatie ervan. Onderdelen hierbij zijn onder andere het opstellen van een impactanalyse en het uitvoeren van testen. Een adequaat Change Management proces waarborgt dat de IT voldoet aan de business eisen. Een specifiek risico in het kader van de jaarrekeningcontrole heeft betrekking op de werking van applications controls die de volledigheid van de te ontvangen premies waarborgen. Hiervoor is een betrouwbare en continue werking van de MAP- en Coda-systemen nodig (zie figuur 2). Met behulp van MAP worden onder meer de te facturen premies berekend, waarna de te ontvangen premies in Coda worden geboekt. Voor de accountant is, in verband met de controle van de jaarrekening, onder meer van belang dat de geïdentificeerde application controls in processen gedurende het jaar goed gewerkt hebben. Elke wijziging op applicatie- of infrastructuurniveau is een potentieel risico dat de betrouwbaarheid of continuïteit kan beïnvloeden. Daarom is het belangrijk om vast te stellen dat wijzigingen geautoriseerd en gestructureerd via het Change Management proces worden doorgevoerd. Dit kan bijvoorbeeld door in het Change Management proces vast te stellen dat testen door programmeurs en gebruikers hebben plaatsgevonden.

Het onderzoek door de accountant en de IT-auditor

Voor de jaarrekeningcontrole heeft de accountant een werkprogramma opgesteld. Naast de financiële controles is in het werkprogramma opgenomen dat de General IT-controls en de application controls onderzocht zullen worden. Voor de controle van de General IT-controls zal hier de controle op het Change Management proces als voorbeeld worden uitgewerkt. Door middel van een goed werkend Change Management proces krijgt de accountant zekerheid over de blijvende goede werking van geprogrammeerde controles, hierdoor kan de accountant zijn controleproces efficiënter én effectiever (minder gegevensgericht) uitvoeren. Op basis van de procesbeschrijving Change Management heeft de IT-auditor een werkprogramma opgesteld, waarbij zowel de opzet als werking van het proces beoordeeld worden. Als onderdeel van de controle van Change Management voert de IT-auditor een deelwaarneming uit op het Change Management proces. Ondermeer de procedure en de key controls (het registreren van verzoeken, de impactanalyse en het testen) worden beoordeeld.

De belangrijkste bevindingen

Op basis van het uitgevoerde onderzoek stelt de IT-auditor vast dat een key control binnen het gehele proces niet gewerkt heeft. Hierdoor zijn wijzigingen, zonder dat deze getest zijn, in productie genomen. Uit nader onderzoek blijkt dat één van de wijzigingen betrekking heeft op een application control in de MAP-applicatie. De application control dient te garanderen dat alle invoer in de basisadministratie MAP volledig worden verwerkt. De IT-auditor heeft vastgesteld dat de controle gedurende drie maanden niet heeft gewerkt.

Naast de bevinding over het testen heeft de IT-auditor nog een aantal opmerkingen bij het proces Change Management. Deze bevindingen zijn verder niet

uitgewerkt. De conclusie van de IT-auditor is dan ook dat beheersmaatregelen onvoldoende hebben gewerkt. Wat betreft de bevinding van de application control is de IT-auditor van mening dat het noodzakelijk is dat de organisatie de aanbeveling opvolgt. Deze uitkomst bespreekt de IT-auditor met de accountant. Hierbij wordt gebruik gemaakt van figuur 2 om inzicht te krijgen in de relatie met de jaarrekeningpost.

3.2 Voorbeeld 2 - Logging op platformniveau

Het risico

Logging op platformniveau is een detectieve beheersmaatregel waarmee de juistheid van acties op platformniveau achteraf kan worden vastgesteld doordat alle gedefinieerde acties worden geregistreerd. Een specifiek risico voor de jaarrekeningcontrole heeft betrekking op de integriteit van data. Om de integriteit van data vast te stellen kan de logging zodanig worden ingesteld dat activiteiten zoals het (al dan niet foutief) inloggen door gebruikers, het uitvoeren van systeemcommando's door beheerders, het wijzigen van autorisaties of het foutlopen van batchverwerkingen worden vastgelegd. De doelstelling van deze logging is het zekerstellen dat geen ongeautoriseerde of onrechtmatige activiteiten worden uitgevoerd op platformniveau.

Het onderzoek door de accountant en de IT-auditor

De IT-auditor doet periodiek onderzoek naar het proces Manage Security. Eén van de elementen hierbij betreft de beoordeling van de logging op platformniveau. Specifiek kijkt de IT-auditor vanuit zijn onderzoek naar de wijze waarop de logging op platformniveau is ingericht, zowel in opzet als werking. Aandachtsgebieden daarbij zijn:

- activiteiten van eindgebruikers die toegang hebben tot het platform;
- activiteiten die beheerders rechtstreeks op het platform uitvoeren;
- activiteiten van applicaties.

De belangrijkste bevindingen

Uit het onderzoek komt naar voren dat de logging op alle servers is geactiveerd. De inrichting van de logging is conform de norm. De lijnorganisatie heeft een controle ingericht om maandelijks de logging te controleren op ongeautoriseerde handelingen. De IT-auditor constateert dat in de maand juli de logging niet is gecontroleerd. De betreffende uitvoerder van de controle was namelijk op vakantie en een vervanger was niet aangesteld. Daarnaast stelt de IT-auditor vast dat tijdens controle door de lijn voor de overige elf maanden geen bijzonderheden zijn geconstateerd.

Op grond van zijn bevindingen komt de IT-auditor tot de conclusie dat voldoende beheersmaatregelen zijn getroffen en dat ze voldoende werken. Wel beveelt hij het management aan (wenselijk) om te waarborgen dat de logging maandelijks wordt gecontroleerd. Deze uitkomst bespreekt de IT-auditor met de accountant, hierbij wordt gebruik gemaakt van figuur 2 om inzicht te krijgen in de relatie met de jaarrekeningpost.

4 De betekenis van de bevindingen voor de jaarrekeningcontrole en de jaarrekening

Op basis van een General IT-controls-onderzoek concludeert de IT-auditor dat een proces niet betrouwbaar is. Hij bespreekt zijn IT-controlebevindingen met de accountant. Samen concluderen zij dat aanvullende werkzaamheden dienen te worden verricht om alsnog voldoende zekerheid te verkrijgen over de betrouwbaarheid van de betreffende jaarrekeningpost.

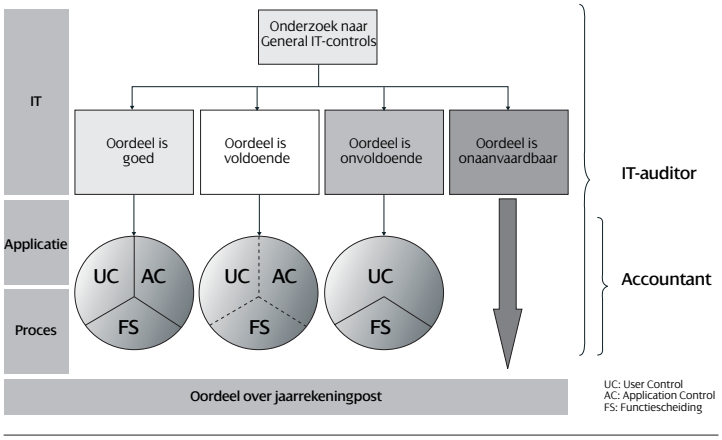
4.1 Generieke modellen

Het model in figuur 3 hanteren wij om de impact van bevindingen op de jaarrekeningcontrole te bepalen.

- **Het oordeel over de General IT-control is goed**

  Uit het onderzoek zijn alleen positieve bevindingen naar voren gekomen. Kenmerken van een 'goed' proces zijn een proactieve beheersing en een continue bewaking. De accountant kan dus op de resultaten van het onderzoek steunen en het is evident dat de werkzaamheden in het kader van de jaarrekeningcontrole op de meest efficiënte wijze kunnen worden uitgevoerd. Hierbij verdeelt de accountant zijn aandacht evenredig over de overige drie controls (user controls, application controls en functiescheiden

Figuur 3 – De betekenis van IT-controlebevindingen op de jaarrekeningcontrole



Figuur 4 De betekenis van oordelen op jaarrekeningposten voor de jaarrekening

Controlebevindingen	Oordeel over jaarrekeningpost	Betekenis voor jaarrekening
Bevindingen alleen positief	Goed	-
Gewenste aanbevelingen	Voldoende	Management letter
Vanaf 1 vereiste aanbeveling	Onvoldoende	Accountantsverslag
Bevindingen alleen negatief	Onaanvaardbaar	Geen goedkeurende accountantsverklaring

ding) om uiteindelijk een oordeel te vormen over de betreffende jaarrekeningpost;

- **Het oordeel over de General IT-control is voldoende**
  Indien één of enkele bevindingen zijn geconstateerd die leiden tot wenselijke opvolging van aanbevelingen, dan leidt dit tot een andere insteek van de controle van de accountant. Kenmerken van een 'voldoende' proces zijn dat het proces informeel dan wel versnipperd wordt uitgevoerd. Ook kunnen proceswerkzaamheden ad hoc plaatsvinden. De accountant zal extra zekerheden willen hebben inzake de gesignaleerde tekortkomingen. De accountant stemt zijn controlemix hierop af;
- **Het oordeel over de General IT-control is onvoldoende**
  In het geval dat minimaal één bevinding is geconstateerd die leidt tot noodzakelijke opvolging van een aanbeveling, zal de accountant aanvullende werkzaamheden uitvoeren ter compensatie. Kenmerken van een 'onvoldoende' proces zijn het ontbreken van inzicht in risico's en managementinformatie. Omdat onvoldoende op de IT kan worden gesteund, zal de accountant de aanvullende werkzaamheden aan de gebruikerskant uitvoeren (user controls). Dit is de minst efficiënte wijze van het uitvoeren van de jaarrekeningcontrole.
- **Het oordeel over de General IT-control is onaanvaardbaar**
  Er zijn alleen negatieve bevindingen geconstateerd. Van een procesinrichting is nauwelijks sprake. Aanvullende werkzaamheden kunnen niet leiden tot compensatie.

In aanvulling op het generieke model voor het bepalen van de impact op de jaarrekeningcontrole hanteren wij een model om op basis van de oordelen over de jaarrekeningposten (onderste blok in figuur 3) de impact op de jaarrekening te bepalen. Dit model is weergegeven in figuur 4. Het oordeel van de jaarrekeningpost is gebaseerd op alle controlebevingen uit de onderzoeken naar de General IT-controls, user controls, application controls en functiescheiding.

4.2 De betekenis van de voorbeelden op de aanpak van de jaarrekeningcontrole

Betekenis IT-controlebevindingen Change Management op de jaarrekeningcontrole

De IT-auditor heeft een aantal General IT-controls onderzocht. Eén daarvan is het Change Management proces. Door niet goed werkende beheersmaatregelen binnen het Change Management proces is geconcludeerd dat niet op de application control (namelijk het automatisch vergelijken van de gegevens uit MAP en Coda) kan worden gesteund. Het is immers niet zeker of de application control de afgelopen periode betrouwbaar heeft gewerkt. Op basis van de uitkomst concludeert de accountant dat hij niet kan steunen op de application controls van de applicatie MAP die het proces Premies ondersteunen. Om toch een oordeel te kunnen geven over de post Premies in de jaarrekening zal de accountant aanvullende werkzaamheden moeten verrichten. De gewenste zekerheid zal de accountant zoeken via de user controls en aanvullende deelwaarnemingen. In overleg met de IT-auditor wordt een aanvullend werkprogramma opgesteld. Naast de application control wordt een standenregister bijgehouden. Maandelijks worden de standen en mutaties vanuit MAP doorgegeven aan Coda. Via het standenregister is het mogelijk om een aansluiting te maken tussen MAP en het standenregister. Aan de IT-auditor wordt de vraag gesteld om een aanvullend onderzoek te doen naar de betrouwbaarheid van het standenregister. Als blijkt dat het standenregister betrouwbaar is, kunnen deze gegevens door de accountant gebruikt worden om een cijferbeoordeling op MAP uit te voeren. Op basis van de uitkomst van de cijferbeoordeling zal de accountant moeten bepalen of hij de post Premies in de jaarrekening goed kan keuren.

Betekenis IT-controlebevindingen Logging op de jaarrekeningcontrole

De IT-auditor heeft een aantal general IT-controls onderzocht. Eén daarvan betreft het loggingproces. Uit het onderzoek is als bevinding gebleken dat de controle door lijnorganisatie op de logging op één maand na maandelijks heeft plaatsgevonden. Omdat uit de controles van de overige 11 maanden geen bijzonderheden zijn gekomen, concludeert de accountant dat hij kan steunen op de betrouwbaarheid van de data die worden gebruikt door de applicatie Coda. Hierdoor kan de accountant zijn controlemix van user controls, application controls en functiescheiding zonder bijzonderheden inrichten.

4.3 De betekenis van de voorbeelden op de jaarrekening

De interpretatie van de IT-controlebevindingen is het uitgangspunt voor het bepalen van de betekenis ervan voor de jaarrekeningcontrole.

Betekenis IT-controlebevindingen Change Managent op de jaarrekening

De accountant zal in ieder geval de vereiste aanbevelingen opnemen in het accountantsverslag en het management wijzen op de noodzaak om de aanbeveling(en) op te volgen.

Betekenis IT-controlebevindingen Logging op de jaarrekening

Hoewel het oordeel van de IT-auditor voldoende is, is ook een wenselijke aanbeveling gedefinieerd om te het waarborgen dat de controle op de logging maandelijks wordt uitgevoerd. Om deze reden zal de accountant de IT-controlebevindingen opnemen in de managementletter, met aanbevelingen ter verbetering van de geconstateerde tekortkomingen.

5 Conclusies

Aan de hand van het model in figuur 5 wordt de betekenis van IT-auditing voor de jaarrekeningcontrole nader ontrafeld. De toegevoegde waarde van General IT-controls onderzoeken laat zich zien in het accountantsverslag en de Management Letter.

- Onderzoeken naar General IT-Controls richten zich op de werking van key controls binnen IT-beheerprocessen. Hiermee kunnen risico's worden gesignaleerd die de betrouwbaarheid van data beïnvloeden. Met alleen de reguliere controlewerkzaamheden van de accountant, komen dergelijke risico's onvoldoende boven tafel.
- De theorie hecht veel waarde aan de betekenis van IT-controlebevindingen voor de jaarrekeningcontrole. Uit de praktijk blijkt dat de impact van IT-controlebevindingen op het accountantsverslag zeer beperkt is. Wij zijn benieuwd naar voorbeelden waar accountants niet tot een goedkeurende accountantsverklaring zijn gekomen, omdat de IT-controlebevindingen daartoe aanleiding gaven.
- Ernstige IT-controlebevindingen worden opgenomen in het jaarlijkse accountantsverslag aan de directie en het auditcommittee van de organisatie. Significante leemtes met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking in het kader van de jaarrekeningcontrole moeten, ingevolge artikel 2:293, lid 4 BW, in het accountantsverslag nader beschreven worden. Overige IT-controlebevindingen vinden hun weg naar de jaarlijkse Management Letter aan de directie van de organisatie.

Figuur 5

De conclusie die wij hieruit trekken is de noodzaak van IT-auditing voor de accountant om enerzijds een volledig risicobeeld te krijgen en anderzijds het efficiënter kunnen uitvoeren van de jaarrekeningcontrole. Maar in de praktijk zien wij geen voorbeelden dat er sprake is van consequenties voor de goedkeuring van de jaarrekening! ■

Literatuur

Boer, J.C., (1999), ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking, in *Compact*, jg. 26, pp. 25-29.

Bommel, C.F. van en H.M. van Goor, (2004), IT-auditing in het kader van de jaarrekeningcontrole?, in *Compact*, jg.31, nr. 2, pp. 10-16.

Bommel, C.F. van en H.M. van Goor, (2005), IT-auditing afbakenen in het kader van de jaarrekeningcontrole, in *Maandblad voor Accountancy en Bedrijfseconomie*, jg.79, nr. 6, pp. 284-292.

Fijneman, R.G.A., (1999), De betekenis en inhoud van 'jaarrekening ICT-Auditing' als onderdeel van de jaarrekeningcontrole; 'Common body of knowledge'- Consequenties voor de accountantscontrole, proefschrift KUB, Tilburg University Press.

IT Governance Institute, (2005), *COBIT, 4.0*, www.itgi.org.

Neisingh, A.W., (2002), Accountantscontrole en informatietechnologie: 'bij elkaar deugen ze niet en van elkaar meugen ze niet', in *Compact*, jg.29, nr 4, pp. 4-11.

Nederlands Instituut van Registeraccountants, Koninklijk (NIVRA), (2005), Richtlijnen voor de Accountantscontrole.

NOREA, (2005), Samenwerking RA-RE inzake de jaarrekeningcontrole, concept versie.

Noot

1 General IT-controls zijn algemene beheersmaatregelen met betrekking tot de automatisering. Voor een nadere uitwerking, zie Van Bommel en Van Goor, 2005; Fijneman, 1999.